ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Review of Data Hiding Techniques

Prof. Sanket .N. Wawale[1], Prof Arindam Dasgupta[2]

[1]Department of Information Technology,
Amrutvahini Polytechnic, Sangamner- 422605, India
[1]sanket.wawale@gmail.com

[2]Department of Information Technology,
Amrutvahini College of Engineering, Sangamner- 422605, India
[2]arindam.dasgupta.family@gmail.com

Abstract: *Information or Data is a very important resource for any organization or individual person. Increase in the number of attack during exchange of information between the source and intended destination has generated a need for a more powerful method for securing data transfer between two entities or storage of data. Cryptography and Steganography are well known and widely used techniques to encode or hide the data. These two techniques has the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. This paper is a survey of different methods of Cryptography and Steganography for Efficient data hiding. For Cryptography different techniques can be used to encode the data. And for Steganography a different medium such as image or audio can be used for hiding the data. Image based Cryptography and Steganography, Wavelet Transform and LSB algorithm has been reviewed in this survey paper. With the help of these two concepts two levels of security can be provided.*

Keywords: *Information Hiding, Cryptography and Steganography*

1. INTRODUCTION

Providing intended access and avoiding un-intended access is a very challenging task. This survey is an approach for studying and analysing security for data provided by using combination of techniques. Un-intended users are threats because they attempt to damage or gain access to certain data by taking advantage of vulnerabilities in the system. For hiding secret information, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used.

Steganography is the art and science of hiding communication and important data. A steganography system thus embeds secret content in unremarkable cover media so that un-authorized user should not be able track or identify the secret data. In the past, people used hidden pictures or invisible ink to convey secret information. Today, computer and network technologies provide easy-to-use communication channels for steganography. Essentially, the information-hiding process in a steganography system starts by identifying a cover medium's redundant bits (those that can be modified without affecting that medium's integrity). The embedding process creates a stego medium by replacing these redundant bits with data or message [1]. Modern steganography's goal is to keep the presence of the message undetectable from an unauthorized access.

2. LITERATURE REVIEW

2.1 Information-Hiding System Features

An information hiding system is characterized by having three different aspects that are related with each other as shown in Figure 1: capacity, security, and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, security refers to inability of Un-authorized user to detect hidden information, and robustness to the amount of modification the stego medium can withstand before showing any negative effects and destroy hidden information [2].

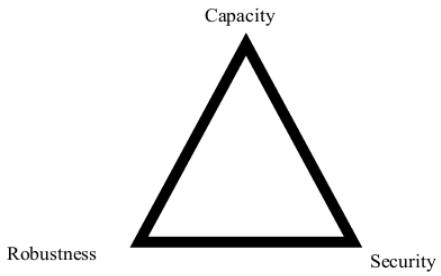

Figure 1: Information Hiding System Features.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Information hiding relates to both watermarking and steganography. A watermarking system's primary goal is to achieve a high level of robustness- that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand, focuses more for high security and capacity, which reveals that the hidden information is easily accessible. Even small modifications to the stego medium can change its meaning.

2.2 Combination of Cryptography & Steganography

Most of the systems today use two levels for providing security for data so that it should not be easy to detect or access the sensitive data. Cryptography is the process of making or converting sensible data into different form. Steganography is the process of Hiding the data into another media file Steganography and Cryptography are two different techniques. Cryptography that involves converting the message so as to make it meaningless to unauthorized people who intercept it. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. According to [6], steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. In addition, the security of classical steganography system relies on secrecy of the data encoding system.

However, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an audio or any other media . The combination of these two methods will enhance the security of the data embedded. This combination of two techniques will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel [7]. The figure 2 and figure 3 below depicts the combination of cryptography and steganography.

2.3 Steganography System:-

A classical steganographic system's security relies on the strength of encoding system. Although such a system might work for a time, if the steganograhy system is known, it is simple enough to expose the entire received media (e.g., images) passing by to check for hidden messages , in such a case steganographic system will collapse.

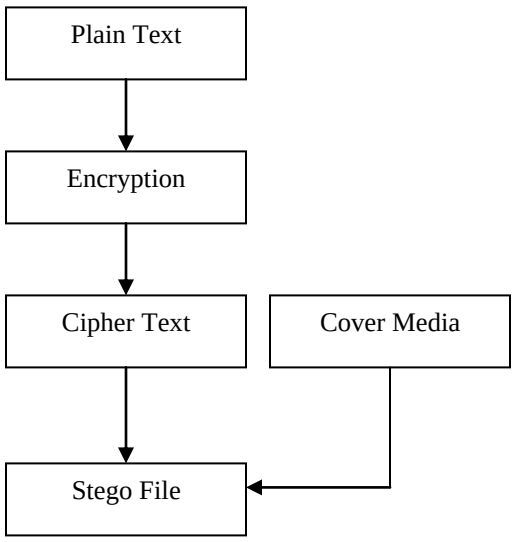

Figure 2: Embedding Data

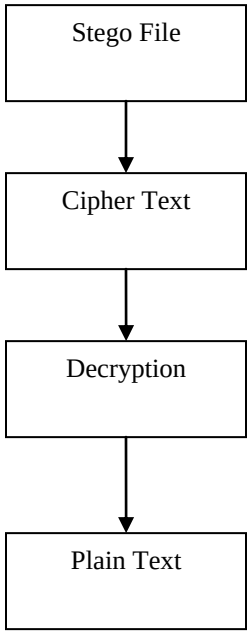

Figure 3: Un-Embedding Data

Modern steganographic system, attempts to be detectable only if secret information is known namely, a secret key. In this case, cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. For steganography to remain undetected, the unmodified cover medium must be kept secret, because if it is exposed, a comparison between

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

the cover and stego media immediately reveals the changes [10].

The Steganography system can be classified into three types:-

- Pure stego systems - no key is used.
- Secret- key stego systems - secret key is used.
- Public - key stego systems - public key is used.

3. REVIEW OF EXISTING TECHNIQUES

3.1 Image Based Hiding

Many techniques have been put forth by researchers for securing electronic communication and data storage. The researchers proposed cryptography and steganography for securing data transfer using images as cover objects for steganography and key for the cryptography. The results of the proposed ISC (Image-Based Steganography and Cryptography) system was presented and the performance of system was compared with F5 algorithm [3]. Also, [4] proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step, finds the shared stego-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the proposed method is that, the sender uses the secret stego-key to select pixels that it will be used to hide. Each selected pixel is then used to hide 8 bits binary information[5] in their research proposed two approaches for secured image steganography using cryptographic techniques and type conversions. One of the methods shows how to secure the image by converting it into cipher text through S-DES algorithm using a secret key and conceal this text in another image using steganography method as shown in figure 4.

The second method shows a new way of hiding an image in another image by encrypting the image directly through S-DES algorithm using a key image and the data obtained is concealed in another image as shown in figure 5.

3.2 The Use of Wavelet Transform in Steganography

A Wavelet is a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying scenario. A signal can be better analyzed if expressed as a linear decomposition of sums of products of coefficient and functions. A two parameter system is constructed such that one has a double sum and coefficient with two indices. The set of coefficients are called the DWT of a signal.

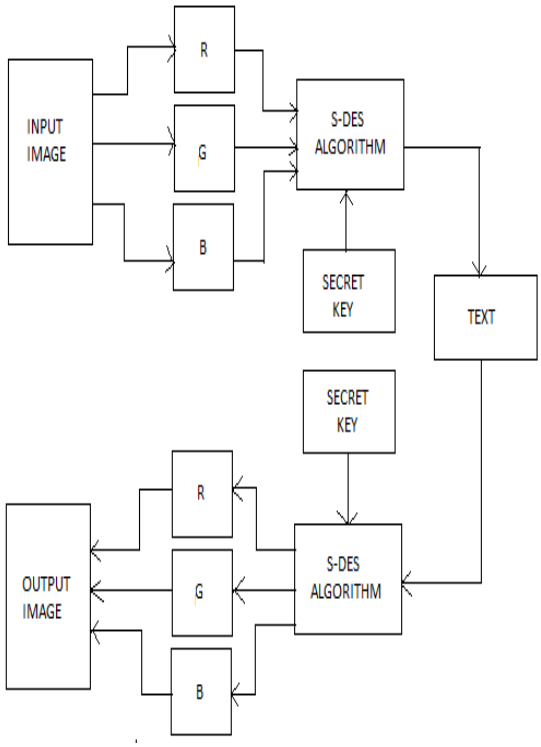

Figure 4: Encryption using Secret Key

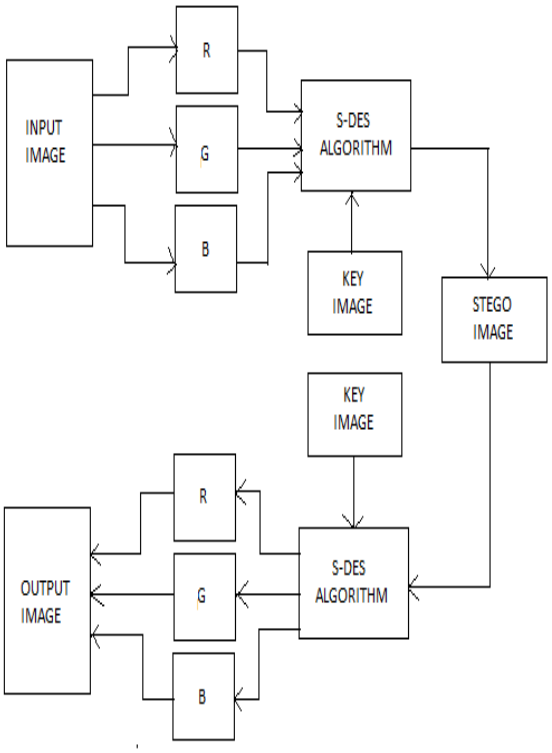

Figure 5: Encryption using Image Key

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

In Wavelet transform, the original signal (1-D,2-D,3-D) is transformed using predefined wavelets. The wavelets are orthogonal, ortho-normal, or biorthogonal, scalar or multi-wavelets [10].

3.2.1 One-Dimensional Wavelet Decomposition

A single-level one dimensional Wavelet decomposition with respect to either a particular Wavelet or particular Wavelet decomposition filters is illustrated in Figure 6. Starting from a signal s, two sets of coefficients are computed: approximation coefficients cA_1, and detail coefficients cD1. These vectors are obtained by convolving s with the low-pass filter Lo_D for approximation and with the high-pass filter Hi_D for detail, followed by dyadic decimation. The length of each filter is equal to 2N. If n is the length of s, the signals F and G are of length n + 2N - 1, and then the coefficients cA_1 and cD_1 are of length [(n-1)/2] +N.

3.2.2 Multilevel 2-D Wavelet Decomposition

For images, an algorithm similar to the one-dimensional case is possible for two- dimensional Wavelets and scaling functions obtained from one-dimensional ones by tensor product [11]. This kind of two-dimensional DWT leads to a decomposition of approximation coefficients at level j in four components: the approximation at level j+1, and the details in three orientations (horizontal, vertical, and diagonal), as depicted in Figure 7.

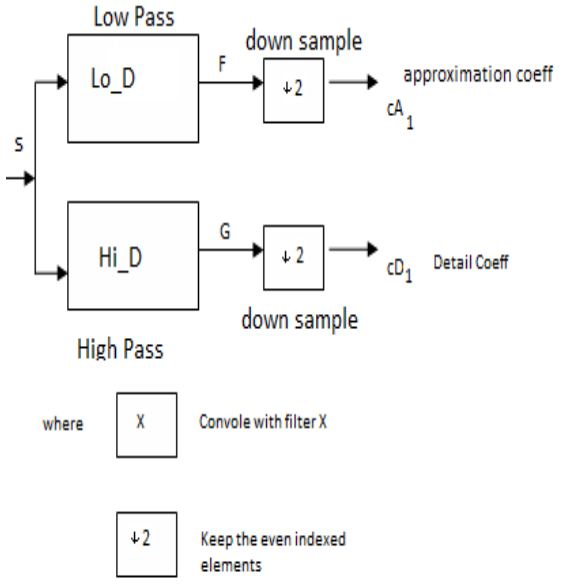

Figure 6: One Dimensional Wavelet Decomposition Filters

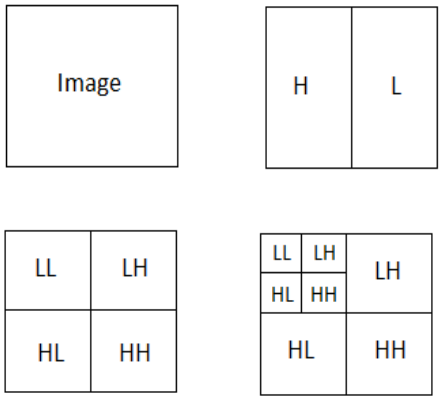

Figure 7: Two Dimensional Wavelet transformation of an image

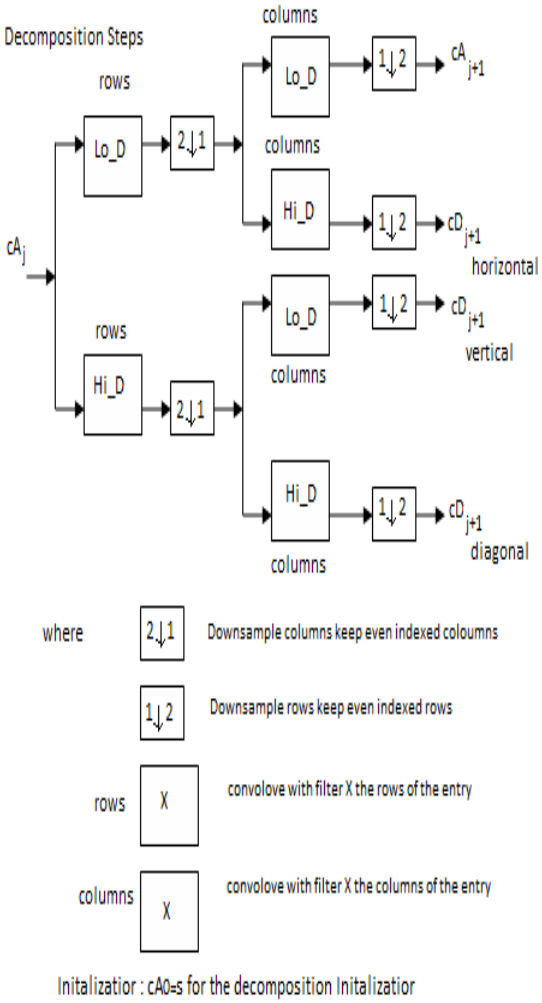

Figure 8: Two Dimensional Wavelet Decomposition

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

Figure 8 describes the basic decomposition step for images using the 2D Wavelet transform. Also, different levels of Wavelet transform were tried. Increasing the levels will add complexity and computational overhead, but the robustness of the steganography method will be increased [10]. Wavelets have been effectively utilized as a powerful tool in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing [10]. Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages that can be gained by using this approach. The use of such transform will mainly address the capacity and robustness of the Information-Hiding system features. The hierarchical nature of the Wavelet representation allows multi-resolution detection of the hidden message, which is a Gaussian distributed random vector added to all the high pass bands in the Wavelet domain. It is shown that when subjected to distortion from compression, the corresponding hidden message can still be correctly identified at each resolution in the Discrete Wavelet Transform (DWT) domain [10]. The DWT can be implemented using the functions available with MATLAB to simplify the analysis and minimize development time.

3.3 Least Significant Bit (LSB)

One of very popular technique is the LSB (Least Significant Bit) algorithm. In this method the least significant bit in some bytes of the cover file are used to hide a sequence of bytes containing the secret data [8]. LSB coding is the simplest way to embed information in a digital audio file by substituting the least significant bit of each sampling points with a binary message. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is some what similar to the least significant digit of a decimal integer, which is the digit in the right-most position. Least significant bits method is frequently used in pseudorandom number generators checksums. In referencing specific bits within a binary number, it is common to assign each bit a bit number, ranging from zero upwards to one less than the number of bits in the number.

4. RESULTS AND DISCUSSION

Following are results of the system that uses LSB algorithm for hiding text in a image and again uses another image for hiding image that contains hidden message [9]. In this example Figure. 9a) shows the original image before the message is stored in it. Figure. 9b) shows the cover image. Here it should be noted that the original image and the cover image are different. The resulting stego image Figure. 9c) is similar to the cover image and is larger in size than the original image.

Figure 9 (a): Original data

Actually what is happening here is that, the data is embedded inside the original image using the LSB algorithm but the image obtained after the embedding process, are distorted so, in order to overcome this limitation distorted image is embedded in a cover image[9].

Figure 9 (b): Cover Image

Figure 9 (c): Stego image file

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

5. CONCLUSION

As per the servey it has been found that cryptography and setganography when used together provides two levels of security for the data. Data hiding wit respect to steganography, three primary objectives are interesting: the technique that will be used for steganography should provide the maximum possible payload, and the embedded data must be imperceptible to the observer. Also the quality of cover media should not be affected after embedding. Image based Cryptography and Steganography is reviewed in this paper. Here compression algorithm is also used with maximum compression ratio of 8 bits/ pixel. It has been tested with few images and different sizes of text files to be hidden and concluded that the resulting stego images do not have any noticeable changes. Also we found that for .bmp images this algorithm works very efficiently [9]. LSB technique for steganography provides easy and effective way for securing the secret data. Wavelet transform allows embedding of the hidden message and reconstruction of the original image. It was found that the proposed method [10] allows high payload (capacity) in the cover image with very little effect on the statistical nature of it.

REFERENCES

[1] Niels, P. And Peter, H 2003. Hide and Seek: An Introduction to Steganography. IEEE Computer Society.IEEE Security and Privacy, pp. 32-44.

[2] Lin T. and Delp J., "A Review of Data Hiding in Digital Images," in Proceedings of the Image Processing, Image Quality, and Image Capture Conference, Georgia, pp. 274-278, 1999.

[3] Efficient Data Hiding System using Cryptography and Steganography Abikoye Oluwakemi C, Adewole Kayode S. , Oladipupo Ayotunde J. -International Journal of Applied Information Systems (IJAIS) ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4 No.11, December 2012

[4] Mohammad, A. A., and Abdelfatah, A. Y. 2010. Public-Key Steganography Based on Matching Method. European Journal of Scientific Research, 40(2). ISSN: 1450-216X. Euro Journals Publishing, Inc., pp. 223-231. Retrieved 21st August, 2012 from http://www.eurojournals.com/ejsr.htm.

[5] Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.

[6] Vivek, J., Lokesh, K., Madhur, M. S., Mohd, S., and Kshitiz Rastogi 2012. Public-Key Steganography Based on Modified LSB Method. Journal of Global Research in Computer Science, 3(4). ISSN: 2229-371X, pp. 26-29.

[7] Raphael, A. J., and Sundaram, V. 2011. Cryptography and Steganography - A Survey. International Journal of Computer Technology Application, 2(3), ISSN: 2229-6093, pp. 626-630.

[8] Jayaram, P., Ranganatha, H. R. and Anupama, H. S. 2011. Information Hiding Using Audio Steganography – A Survey. International Journal of Multimedia and Its Application, 3(3), pp. 86-96.

[9] A New Approach to Hide Text in Images Using Steganography-Vipul Sharma, Sunny Kumar-IJARCSSE-ISSN: 2277 128X, Volume 3, Issue 4, April 2013.

[10]"A Modified High Capacity Image Steganography Technique Based on Wavelet Transform"-Ali AlAtaby, Fawzi Al Naima-The International ArabJournal of In-formation Technology, Vol. 7, No. 4, October 2010.

[11] Johnson N. And Jajodia S., "Steganography: Seeing the Unseen," IEEE Computer Magazine, vol. 25, no. 4, pp. 26-34, 1998.